ACNS
CCSN

Advisory Committee on Nuclear Safety
Comité consultatif de la sûreté nucléaire

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9
Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

COMMITTEE REPORTS

Since the 1950's the Atomic Energy Control Board has made use of advisory committees of independent experts to assist it in its decision-making process. In 1979 the Board restructured the organization of these consultative groups, resulting in the creation of two senior level scientific committees charged with providing the Board with independent advice on principles, standards and general practices related to radiation protection and the safety of nuclear facilities. The two committees are the Advisory Committee on Radiological Protection (ACRP), formed in 1979, and the Advisory Committee on Nuclear Safety (ACNS), which was established a year later. Summaries of meetings of the committees are available to the public in the AECB library in Ottawa.

From time to time the committees issue reports which are normally published by the AECB and catalogued within the AECB's public document system. Committee reports, bound with a distinctive cover, carry both a committee-designated reference number, e.g. ACRP-1, and an AECB reference number in the "INFO" series. The reports generally fall into two broad categories: (i) recommendations to the Board on a particular technical topic, and (ii) background studies. **Unless specifically stated otherwise, publication by the AECB of a committee report does not imply endorsement by the Board of the content, nor acceptance of any recommendations made therein.**

RAPPORTS DES COMITÉS

Depuis les années cinquante, la Commission de contrôle de l'énergie atomique fait appel à des comités consultatifs composés d'experts indépendants pour l'aider dans ses prises de décision. En 1979, la CCEA a restructuré l'organisation de ces groupes de consultation pour former deux comités scientifiques supérieurs chargés de lui fournir des conseils indépendants concernant les principes, les normes et les méthodes générales touchant la radioprotection et la sûreté des installations nucléaires : ce sont le Comité consultatif de la radioprotection (CCRP), formé en 1979, et le Comité consultatif de la sûreté nucléaire (CCSN), établi l'année suivante. Le public peut consulter les comptes rendus des réunions de ces comités à la bibliothèque de la CCEA, à Ottawa.

Les comités rédigent à l'occasion des rapports qui sont normalement publiés par la CCEA et catalogués dans la collection des documents publics de la CCEA. Reliés avec une couverture distincte, les rapports des comités se reconnaissent à leur numéro de référence du comité d'origine (comme CCRP-1) et à leur numéro de référence de la CCEA dans la série «INFO». Ils se divisent habituellement en deux catégories générales : (i) les recommandations présentées à la Commission au sujet d'une question technique particulière; (ii) les études générales. **À moins d'indication contraire, la publication par la CCEA du rapport d'un comité ne signifie pas que la Commission approuve le contenu de la publication, ni qu'elle en accepte les recommandations.**

INFO-0404

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

ACNS-19

RECOMMENDATIONS RELATING TO SAFETY-CRITICAL REAL-TIME SOFTWARE IN NUCLEAR POWER PLANTS

by the

Advisory Committee on
Nuclear Safety

January 1992

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

ABSTRACT

The Advisory Committee on Nuclear Safety (ACNS) has reviewed safety issues associated with the software for the digital computers in the safety shutdown systems for the Darlington NGS. From this review the ACNS has developed four recommendations for safety-critical real-time software in nuclear power plants. These recommendations cover:

- the completion of the present efforts to develop an overall standard and sub-tier standards for safety-critical real-time software;
- the preparation of schedules and lists of responsibilities for this development;
- the concentration of AECB efforts on ensuring the scrutability of safety-critical real-time software; and
- the collection of data on reliability and causes of failure (error) of safety-critical real-time software systems and on the probability and causes of common-mode failures (errors).

TABLE OF CONTENTS

Page

ABSTRACT

1. INTRODUCTION 1

2. SCOPE 1

3. DISCUSSION 2

4. RECOMMENDATIONS 3

References 5

Acknowledgements 6

RECOMMENDATIONS RELATING TO SAFETY-CRITICAL REAL-TIME SOFTWARE IN NUCLEAR POWER PLANTS

1. INTRODUCTION

The Advisory Committee on Nuclear Safety (ACNS) first considered the use of digital computers in a reactor safety system early in 1981, when AECB President J.H.F. Jennekens asked the Committee for its views on an Ontario Hydro (OH) proposal to use digital, programmable, computers in the shutdown systems of the Darlington Nuclear Generating Station [1].

The ACNS presented its report [2] in June 1981 concluding that no fundamental principle would be challenged by the introduction of computer technology into the safety systems. However, some concerns were noted having to do with the need for control of software quality, provision of documentation that would permit an independent and meaningful review, and administrative controls over in-service modifications.

At a meeting of the Joint Subcommittee on Regulatory Research in December 1988 we were told, during a discussion on research priorities, that the review of software for the Darlington shutdown systems was the major licensing problem facing the Board staff at that time. As a result, the ACNS decided to review the problem in some detail.

It was soon apparent, however, that the various organizations (AECL, OH, AECB) with whom the ACNS would want to meet were too busy reviewing the Darlington shutdown systems software to spend time with the Committee so the review was put on hold. By the time the review was resumed in mid-1990 the software for both shutdown systems at Darlington had been approved for use (in the short term), after a lengthy review and audit process, and the preparation of software standards was being undertaken by Ontario Hydro, AECL and the staff of the AECB. Since the AECB has instructed Ontario Hydro to re-design the Darlington NGS safety systems software in order to facilitate review of any proposed future modifications, but has also stipulated that any re-design await completion and acceptance of the software standards, the ACNS has decided to review the progress being made on these activities and make whatever recommendations seem appropriate.

2. SCOPE

There are many safety-related computer programs associated with the design and operation of nuclear facilities. Of those that operate in real time, the following have been the subject of much discussion between AECB staff and licensees:

i) Safety computer software that accepts inputs from process instruments and other sources and generates plant protection action signals in real time directly as a result of unsupervised internal processing. (The trip computer software)

ii) Control computer software that accepts inputs from process instruments and other sources and generates plant control action signals in real time directly as a result of unsupervised internal processing. (This could be software for reactor control or for fuelling machine control.)

iii) Display computer software that accepts data from the protection system or the control system and generates, in real time, alarms, control panel displays, etc. It may also interact with either system by transmitting data to it. This interaction could be the changing of action levels or the initiation of test procedures.

The ACNS has concentrated on the first one above.

3. DISCUSSION

On March 29, 1990, Ontario Hydro presented to the ACNS an overview of the review process that led to approval of the Darlington software by the AECB. In addition, an ACNS working group met on several occasions later in the year with Ontario Hydro, AECL Engineering, and the AECB staff to learn of the progress being made in the production of standards and regulatory guides relevant to safety-critical software.

It became evident that the current design of the Darlington shutdown systems had started with no agreed-upon software standards in place although the designer did have some in-house programming guidelines and draft versions of the CAN/CSA - Q396.1 and .2 series of standards for quality assurance [3, 4, 5, 6], eventually published in final form in January 1989. These were apparently not considered adequate by the AECB and a lengthy review and audit process ensued. In order to avoid a repetition of this process, should any significant future modification to the software be required, Ontario Hydro and AECL are collaborating to produce a set of software standards based largely on the experience gained by both the designer and the AECB (aided by several software consultants) during the detailed review process to which the Darlington software was subjected. While there are many software standards already available (30 or so were reviewed by Ontario Hydro) only the International Electrotechnical Commission (IEC) Standard [7], Publication 880, was found to be of significant value by Ontario Hydro as a basis for this work. An overall standard [8] has now been prepared by Ontario Hydro and AECL. It is intended to be sufficiently general to deal with the various categories of safety-related software listed above and is currently undergoing trial use to establish its adequacy.

In addition to the overall standard, a set of sub-tier standards will be required to provide more detail specific to the various categories of software. Also required will be the development of methodologies for carrying out many of the activities to be covered by the new standards. Ontario Hydro has estimated that approximately three years will be required to develop these standards and to obtain AECB endorsement, although this estimate may be optimistic. This effectively defines the "short term" approval mentioned in section 1, for the Darlington shutdown systems software as covering a period of at least 4-5 years.

The ACNS has suggested to AECB staff and Ontario Hydro that they obtain precise quantitative software reliability data on existing systems that are being used in safety critical situations by the nuclear industry both in Canada and in other countries (USA, UK, and France, for example), but no initiatives appear to be underway. It is felt that such data might give a more balanced view of software reliability than the few anecdotal pieces of information that are now used to characterize it. In this connection it is important to recognize that software quality assurance does not have to eliminate all errors, any more than hardware quality assurance has to eliminate all faults in the equipment that the software replaces. The principle of defence-in-depth allows for the fact that hardware fails, that humans err, that acts of God occur... and that software can contain some errors.

The ACNS also discussed the manner in which the principle of diversity is being applied to the software in each of the two Darlington shutdown systems. The objective of diversity is to reduce to an acceptable level the possibility of a common-mode failure of the total fast shutdown function. In keeping with the existing hardware diversity, the software for each of the two systems has been written by different engineers using different programming languages. However, one of the software consultants retained by AECB staff cites experimental evidence [9] that different software designers given the same task will make similar errors and so will negate to some extent the attempt to make the systems diverse. This situation should be carefully reviewed and an attempt made to get some quantitative measure of the probability that a software error (e.g. a mistake in specification, design, or implementation) common to both shutdown systems might prevent them from detecting or responding to an accident situation requiring a plant shutdown.

4. RECOMMENDATIONS

There is an urgent need for CSA standards for safety critical software to be in place so that future applications of this technology, which is so important in the critical area of reactor safety, can proceed from a sound regulatory base. It is recommended that

(1) ***The Atomic Energy Control Board encourage its staff to work expeditiously with the nuclear industry towards completing an overall standard and sub-tier standards for safety-critical real-time software for nuclear power plants and issuing them as nuclear standards through the Canadian Standards Association consensus process.***

It would aid the Board and its Advisory Committees in following the progress of this standards development work if a schedule of activities were available. Therefore, it is recommended that

(2) ***The AECB encourage its staff to seek the cooperation of the nuclear industry in preparing a schedule showing the documents to be prepared to guide the development of safety-critical real-time software, the party responsible for the preparation of each document, and the expected time of completion of each document.***

It is appreciated that AECB staff and its consultants have strongly influenced the contents of the Ontario Hydro overall standard [8] and that they will continue to influence the sub-tier standards still to come. However, it is recommended that

(3) *The AECB, in defining its own requirements and preference as regulatory policy statements and regulatory guides, concentrate on ensuring that the designers' software programs will be scrutable by the AECB with a reasonable amount of effort.*

In reviewing the anecdotal accounts of so-called "software failures", the ACNS has not, in most cases, been able to identify what precisely "failed". It suspects that most often the fault was a deficiency in the design of the software and that the software was doing exactly what it was designed to do, i.e. it was highly reliable. Furthermore, as noted in section 3, there is some experimental evidence that may support this suspicion, namely, that different software designers given the same task will make similar errors. Therefore, it is recommended that

(4) *The AECB obtain, or urge the industry to obtain, precise quantitative reliability data and causes of failure for safety-critical real-time software systems now being used in the nuclear industry in Canada and elsewhere, and carefully examine the probability of common-mode failures and their causes.*

References

1. Letter, J.H. Jennekens, President, Atomic Energy Control Board, to Dr. H.E. Duckworth, Chairman, ACNS, 14 January 1981.

2. ACNS-3, "A Report on the Use of Programmable Digital Computers in the Shutdown of the Darlington G.S.", June 1981. (AECB INFO-0056)

3. CAN/CSA-Q396.1.1-89, "Quality Assurance Program for the Development of Software Used in Critical Applications".

4. CAN/CSA-Q396.1.2-89, "Quality Assurance Program for Previously Developed Software Used in Critical Applications".

5. CAN/CSA-Q396.2.1-89, "Quality Assurance Program for the Development of Software Used in Noncritical Applications".

6. CAN/CSA-Q396.2.2-89, "Quality Assurance Program for Previously Developed Software Used in Noncritical Applications".

7. IEC Standard, Publication 880, "Software for Computers in the Safety Systems of Nuclear Power Plants", International Electrotechnical Commission, First Edition 1986.

8. 982 C-H 69002-0001 Rev. 00, "Standard for Software Engineering of Safety Critical Software", Ontario Hydro, December 21, 1990.

9. J. Knight and N. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multiversion Programming", IEEE Transactions on Software Engineering, January 1986.

Acknowledgements

Members of the Working Group:

A. Pearson, Chairman
Y.M. Giroux
O.R. Lundell
J.T. Rogers

Members of the Secretariat assisting:

R.J. Atchison
E. Daigle (typing)

All the members of the Advisory Committee on Nuclear Safety.

ACNS
CCSN

Advisory Committee on Nuclear Safety
Comité consultatif de la sûreté nucléaire

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9
Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

COMMITTEE REPORTS

Since the 1950's the Atomic Energy Control Board has made use of advisory committees of independent experts to assist it in its decision-making process. In 1979 the Board restructured the organization of these consultative groups, resulting in the creation of two senior level scientific committees charged with providing the Board with independent advice on principles, standards and general practices related to radiation protection and the safety of nuclear facilities. The two committees are the Advisory Committee on Radiological Protection (ACRP), formed in 1979, and the Advisory Committee on Nuclear Safety (ACNS), which was established a year later. Summaries of meetings of the committees are available to the public in the AECB library in Ottawa.

From time to time the committees issue reports which are normally published by the AECB and catalogued within the AECB's public document system. Committee reports, bound with a distinctive cover, carry both a committee-designated reference number, e.g. ACRP-1, and an AECB reference number in the "INFO" series. The reports generally fall into two broad categories: (i) recommendations to the Board on a particular technical topic, and (ii) background studies. **Unless specifically stated otherwise, publication by the AECB of a committee report does not imply endorsement by the Board of the content, nor acceptance of any recommendations made therein.**

RAPPORTS DES COMITÉS

Depuis les années cinquante, la Commission de contrôle de l'énergie atomique fait appel à des comités consultatifs composés d'experts indépendants pour l'aider dans ses prises de décision. En 1979, la CCEA a restructuré l'organisation de ces groupes de consultation pour former deux comités scientifiques supérieurs chargés de lui fournir des conseils indépendants concernant les principes, les normes et les méthodes générales touchant la radioprotection et la sûreté des installations nucléaires : ce sont le Comité consultatif de la radioprotection (CCRP), formé en 1979, et le Comité consultatif de la sûreté nucléaire (CCSN), établi l'année suivante. Le public peut consulter les comptes rendus des réunions de ces comités à la bibliothèque de la CCEA, à Ottawa.

Les comités rédigent à l'occasion des rapports qui sont normalement publiés par la CCEA et catalogués dans la collection des documents publics de la CCEA. Reliés avec une couverture distincte, les rapports des comités se reconnaissent à leur numéro de référence du comité d'origine (comme CCRP-1) et à leur numéro de référence de la CCEA dans la série «INFO». Ils se divisent habituellement en deux catégories générales : (i) les recommandations présentées à la Commission au sujet d'une question technique particulière; (ii) les études générales. **À moins d'indication contraire, la publication par la CCEA du rapport d'un comité ne signifie pas que la Commission approuve le contenu de la publication, ni qu'elle en accepte les recommandations.**

INFO-0404

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

CCSN-19

RECOMMANDATIONS RELATIVES AUX LOGICIELS EN TEMPS RÉEL CRITIQUES POUR LA SÛRETÉ DANS LES CENTRALES NUCLÉAIRES

par le

Comité consultatif de la
sûreté nucléaire

Janvier 1992

RÉSUMÉ

Le Comité consultatif de la sûreté nucléaire (CCSN) a étudié les questions de sûreté associées aux logiciels pour les ordinateurs numériques des systèmes d'arrêt d'urgence pour la centrale nucléaire Darlington. Cette étude a débouché sur quatre recommandations pour un logiciel en temps réel critique pour la sûreté dans les centrales nucléaires portant sur ce qui suit :

- l'achèvement des travaux actuels d'élaboration d'une norme d'ensemble et de normes auxiliaires pour un logiciel en temps réel critique pour la sûreté;
- la préparation d'échéanciers et de listes de responsabilités pour cette élaboration;
- la concentration des efforts de la CCEA pour s'assurer qu'un logiciel en temps réel critique pour la sûreté puisse être examiné, et
- la collecte de données sur la fiabilité et les causes de défaillance (erreur) des systèmes de logiciel en temps réel critique pour la sûreté et sur la probabilité et les causes des défaillances en mode commun (erreurs).

TABLE DES MATIÈRES

Page

RÉSUMÉ

1. INTRODUCTION 1

2. PORTÉE 1

3. DISCUSSION 2

4. RECOMMANDATIONS 3

Bibliographie 5

Remerciements 6

RECOMMANDATIONS RELATIVES AUX LOGICIELS EN TEMPS RÉEL CRITIQUES POUR LA SÛRETÉ DANS LES CENTRALES NUCLÉAIRES

1. INTRODUCTION

Le Comité consultatif de la sûreté nucléaire (CCSN) a tout d'abord envisagé l'utilisation d'ordinateurs numériques dans un système de sûreté de réacteur en 1981, alors que le président de la CCEA, J.H.F. Jennekens, demanda au Comité son opinion sur une proposition d'Ontario Hydro (OH) visant l'utilisation d'ordinateurs numériques programmables dans les systèmes d'arrêt de la centrale nucléaire Darlington [1].

Le CCSN a présenté son rapport [2] en juin 1981, dont la conclusion était qu'aucun principe fondamental ne serait remis en cause advenant l'utilisation de la technologie de l'informatique dans les systèmes de sûreté. Certaines préoccupations avaient toutefois été soulevées concernant la nécessité d'un contrôle de la qualité du logiciel, la fourniture de documentation qui permettrait un examen indépendant et significatif ainsi que le contrôle administratif sur les modifications apportées en cours d'exploitation.

Lors d'une réunion du sous-comité mixte sur les études normatives en décembre 1988, les membres ont été informés dans le cadre d'une discussion sur les priorités de recherche, que l'étude des logiciels pour les systèmes d'arrêt de Darlington constituait le principal problème d'autorisation que devait affronter le personnel de la CCEA à ce moment. Par conséquent, le CCSN a décidé d'examiner le problème de façon assez approfondie.

Il est toutefois vite devenu manifeste que les divers organismes (EACL, OH, CCEA) que le CCSN voudrait rencontrer étaient trop occupés à examiner les logiciels des systèmes d'arrêt pour consacrer du temps au Comité, de sorte que l'examen du problème a été suspendu. Lorsque l'étude a été reprise au milieu des années 1990, l'utilisation des logiciels pour les deux systèmes d'arrêt à Darlington avait été approuvée (à court terme) après un long processus d'examen et de vérification et la préparation de normes de logiciel était entreprise par Ontario Hydro, l'EACL, l'ACNOR et le personnel de la CCEA. Puisque la CCEA a demandé à Ontario Hydro de reprendre la conception des logiciels des systèmes de sûreté de la centrale nucléaire Darlington en vue de faciliter l'examen de toute modification future proposée, en stipulant que toute nouvelle conception était sujette à l'achèvement et à l'acceptation des normes de logiciel, le CCSN a décidé d'examiner les progrès accomplis jusqu'à maintenant concernant ces activités et de formuler toute recommandation pertinente.

2. PORTÉE

Il existe de nombreux programmes de logiciel reliés à la sûreté et associés à la conception et à l'exploitation d'installations nucléaires. Parmi ceux qui fonctionnent en temps réel, les logiciels suivants ont fait l'objet de beaucoup de discussion entre le personnel de la CCEA et les détenteurs d'un permis d'exploitation :

i) Le logiciel de sûreté qui accepte des données des instruments de traitement et d'autres sources et produit des signaux d'intervention de

protection de la centrale en temps réel découlant de façon directe d'un traitement interne non supervisé. (Le logiciel de déclenchement.)

ii) Le logiciel de contrôle qui accepte des données des instruments de traitement et d'autres sources et produit des signaux d'intervention de contrôle en temps réel découlant de façon directe d'un traitement interne non supervisé. (Il pourrait s'agir d'un logiciel de contrôle du réacteur ou de contrôle de l'appareil d'alimentation.)

iii) Le logiciel d'affichage qui accepte des données du système de contrôle ou de protection et produit, en temps réel, des affichages de tableau de commande, des signaux d'alerte, etc. Il peut aussi dialoguer avec l'un ou l'autre système en leur transmettant des données. Ce dialogue pourrait toucher le changement des niveaux d'intervention ou la mise en oeuvre de procédés d'essai.

Le CCSN s'est concentré sur le premier logiciel mentionné.

3. DISCUSSION

Le 29 mars 1990, Ontario Hydro présentait au CCSN un aperçu du processus d'examen qui a mené à l'approbation du logiciel de Darlington par la CCEA. En outre, un groupe de travail du CCSN a rencontré, à plusieurs reprises, plus tard dans l'année, Ontario Hydro, l'EACL (CANDU) et le personnel de la CCEA pour se tenir au courant des progrès accomplis concernant la production de normes et de guides de réglementation pertinentes à un logiciel critique pour la sûreté.

Il devint évident que la conception actuelle des systèmes d'arrêt de Darlington avait commencé au début des années 1980 sans normes convenues de logiciel, quoique le concepteur possédait certaines lignes directrices internes de programmation et une version provisoire de la série de normes CAN/CSA - Q396.1 et .2 pour l'assurance de la qualité [3, 4, 5, 6], normes par la suite publiées dans leur forme définitive en janvier 1989. Il semble que la CCEA ne considérait pas ces normes adéquates et un long processus d'examen et de vérification s'en est suivi. Pour éviter de revivre une telle expérience, au cas où une importante modification future du logiciel s'imposerait, Ontario Hydro et EACL travaillent en collaboration à la production d'une série de normes de logiciel fondées en grande partie sur l'expérience acquise tant par le concepteur que par la CCEA (aidée par plusieurs experts-conseils en logiciels) pendant l'examen détaillé du logiciel de Darlington. Bien qu'il existe déjà de nombreuses normes relatives au logiciel (Ontario Hydro en a examiné environ une trentaine), Ontario Hydro n'en a trouvé qu'une seule d'une valeur appréciable comme fondement pour ses travaux, soit la norme [7], publication 880, de la Commission électrotechnique internationale (CEI). Ontario Hydro et EACL ont maintenant rédigé une norme globale [8], qu'on prévoit suffisamment générale pour traiter des diverses catégories de logiciel relié à la sûreté susmentionnées et elle est actuellement à l'essai pour déterminer sa justesse.

En plus de la norme globale, il faudra rédiger une série de normes auxiliaires s'appliquant plus en détail aux diverses catégories de logiciel. Il faudra en outre élaborer des méthodologies pour réaliser bon nombre des activités traitées par les nouvelles normes. Ontario Hydro a estimé que l'élaboration de ces normes

et leur approbation par la CCEA nécessiteront environ trois ans, quoique cette estimation puisse être optimiste. Ceci, effectivement, définit l'approbation à «court terme» mentionnée à la section 1, pour les logiciels des systèmes d'arrêt à Darlington, comme une approbation couvrant une période d'au moins 4-5 ans.

Quant à la réglementation, des documents devront être rédigés pour établir les exigences qui assureront que les programmes de logiciel pourront être examinés par la CCEA.

Le CCSN a suggéré au personnel de la CCEA et à Ontario Hydro d'obtenir des données quantitatives précises de fiabilité de logiciel sur les systèmes établis employés dans des situations critiques pour la sûreté par l'industrie nucléaire tant au Canada que dans d'autres pays (États-Unis, Royaume-Uni et France par exemple), mais il semble n'y avoir aucune initiative en cours. Le CCSN croit que ce type de données pourrait donner une vision plus équilibrée de la fiabilité de logiciel que les quelques renseignements anecdotiques actuellement utilisés pour la caractériser. À ce propos, il est important de reconnaître que l'assurance-qualité de logiciel n'a pas à éliminer toutes les erreurs, tout comme l'assurance-qualité de matériel n'a pas à éliminer toutes les erreurs du matériel que le logiciel remplace. Le principe de défense en profondeur tient compte du fait que le matériel tombe en panne, que les humains font des erreurs, que des cas de force majeure peuvent survenir...et que le logiciel peut contenir des erreurs.

Le CCSN a également discuté de la façon dont le principe de la diversité est appliqué au logiciel dans chacun des deux systèmes d'arrêt de Darlington. L'objectif de la diversité est de réduire à un niveau acceptable la possibilité d'une défaillance en mode commun de la fonction d'arrêt rapide total. Compte tenu de la diversité du matériel actuel, le logiciel utilisé pour chacun des deux systèmes a été écrit par différents ingénieurs utilisant différents langages de programmation. Toutefois, un des conseillers en logiciel dont les services ont été retenus par le personnel de la CCEA cite une évidence expérimentale [9] selon laquelle différents concepteurs de logiciel ayant la même tâche feront des erreurs semblables et annuleront donc dans une certaine mesure la tentative de diversifier les systèmes. Cette situation devrait être soigneusement examinée et on devrait essayer d'obtenir une certaine mesure quantitative de la probabilité qu'une erreur de logiciel (par ex. une erreur de spécification, de conception ou de mise en application) commune aux deux systèmes d'arrêt pourrait empêcher la détection d'une situation d'accident exigeant un arrêt de la centrale.

4. RECOMMANDATIONS

Il est urgent que l'ACNOR adopte des normes sur le logiciel critique pour la sûreté, afin que les applications futures de cette technologie, d'une telle importance dans le domaine crucial de la sûreté des réacteurs, puissent se fonder sur une base réglementaire solide. Il est recommandé

(1) ***Que la Commission de contrôle de l'énergie atomique encourage son personnel à collaborer de façon diligente avec l'industrie nucléaire afin d'élaborer une norme globale et des normes auxiliaires sur le***

logiciel en temps réel critique pour la sûreté dans les centrales nucléaires et de les publier à titre de normes nucléaires par l'entremise du processus de consensus de l'Association canadienne de normalisation.

La Commission et ses comités consultatifs pourraient plus facilement suivre les travaux d'élaboration des normes avec un calendrier des activités. Il est donc recommandé

(2) *Que la CCEA encourage son personnel à solliciter la coopération de l'industrie nucléaire en vue de dresser un calendrier indiquant les documents à préparer pour orienter la mise au point de logiciel en temps réel critique pour la sûreté, les parties responsables de la préparation de chaque document et le délai prévu de préparation desdits documents.*

Le CCSN est conscient que le personnel et les experts-conseils de la CCEA ont fortement influencé le contenu de la norme globale d'Ontario Hydro [8] et qu'ils influenceront les normes auxiliaires à venir. Toutefois le CCSN recommande

(3) *Que la CCEA, dans la définition de ses exigences et préférences sous forme d'énoncés de politique réglementaire et de guides réglementaires, s'assure que les logiciels des concepteurs puissent être examinés par la CCEA moyennant des efforts raisonnables.*

Dans l'examen de comptes rendus anecdotiques de soi-disant «défaillances de logiciel», le CCSN n'a pas réussi, dans la plupart des cas, à définir la nature de la «défaillance». Le CCSN soupçonne que, la plupart du temps, la défaillance provenait d'un défaut dans la conception du logiciel et que ce logiciel fonctionnait en fait exactement comme prévu, c'est-à-dire qu'il était très fiable. De plus, tel que mentionné à la section 3, il y a une certaine évidence expérimentale qui appuie ce soupçon, à savoir que des concepteurs différents s'acquittant de la même tâche peuvent effectuer la même erreur. C'est pourquoi il est recommandé

(4) *Que la CCEA obtienne ou incite l'industrie à obtenir, des données quantitatives précises sur la fiabilité et les causes de défaillance des logiciels en temps réel critiques pour la sûreté actuellement en usage dans l'industrie nucléaire au Canada et à l'étranger, afin d'étudier soigneusement les probabilités de défaillances en mode commun et leurs causes.*

Bibliographie

1. Lettre, J.H. Jennekens, President, Atomic Energy Control Board, à Dr. H.E. Duckworth, Chairman, ACNS, 14 janvier 1981.

2. CCSN-3, «Rapport sur l'utilisation d'ordinateurs numériques programmables dans les systèmes d'arrêt de la centrale de Darlington», juin 1981 (CCEA-INFO-0056(F))

3. CAN/CSA-Q396.1.1-89, «Programme d'assurance de la qualité pour la réalisation de logiciels critiques», janvier 1989.

4. CAN/CSA-Q396.1.2-89, «Programme d'assurance de la qualité pour les logiciels critiques en service», janvier 1989.

5. CAN/CSA-Q396.2.1-89, «Programme d'assurance de la qualité pour la réalisation de logiciels non critiques», janvier 1989.

6. CAN/CSA-Q396.2.2-89, «Programme d'assurance de la qualité pour les logiciels non critiques en service», janvier 1989.

7. Norme de la CEI, Publication 880, «Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires», Commission électrotechnique internationale, première édition, 1986.

8. 982 C-H 69002-0001 Rev. 00, "Standard for Software Engineering of Safety Critical Software", Ontario Hydro, 21 décembre 1990.

9. J. Knight et N. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multiversion Programming", IEEE Transactions on Software Engineering, janvier 1986.

Remerciements

Membres du Groupe de travail :

A. Pearson, président
Y.M. Giroux
O.R. Lundell
J.T. Rogers

Membres du Secrétariat ayant apporté leur soutien :

R.J. Atchison
E. Daigle (dactylographie)

Tous les membres du Comité consultatif de sûreté nucléaire